DNSで潜在的なプロパガンダツールの存在を調査

目次

要旨

The Citizen Labが最近、ヨーロッパ、アジアおよびラテンアメリカの30カ国で報道機関を標的に展開された「PAPERWALL」というオンライン上のプロパガンダキャンペーンを発見しました。

PAPERWALLは、Mandiantが2023年7月に報告したインフルエンスオペレーションの「HaiEnergy」と共通している点があります。PAPERWALLもHaiEnergyも、Times Newswireからコンテンツのかなりの部分を引用していたのです。しかし、PAPERWALLの運用者はHaiEnergyのそれとは違っており、また独自のツール、戦術、技術および手順（TTP）を有しているという点でも両者は異なっていました。

WhoisXML APIの研究者はこのほど、DNSインテリジェンスを活用してPAPERWALLの痕跡を詳細に調査しました。具体的には、The Citizen Labが公表したPAPERWALLのセキュリティ侵害インジケーター（IoC）132個（ドメインIoC 123個およびIPアドレスIoC 9個）を分析しました。その結果、以下のPAPERWALL関連のアーティファクトを新たに発見しました：

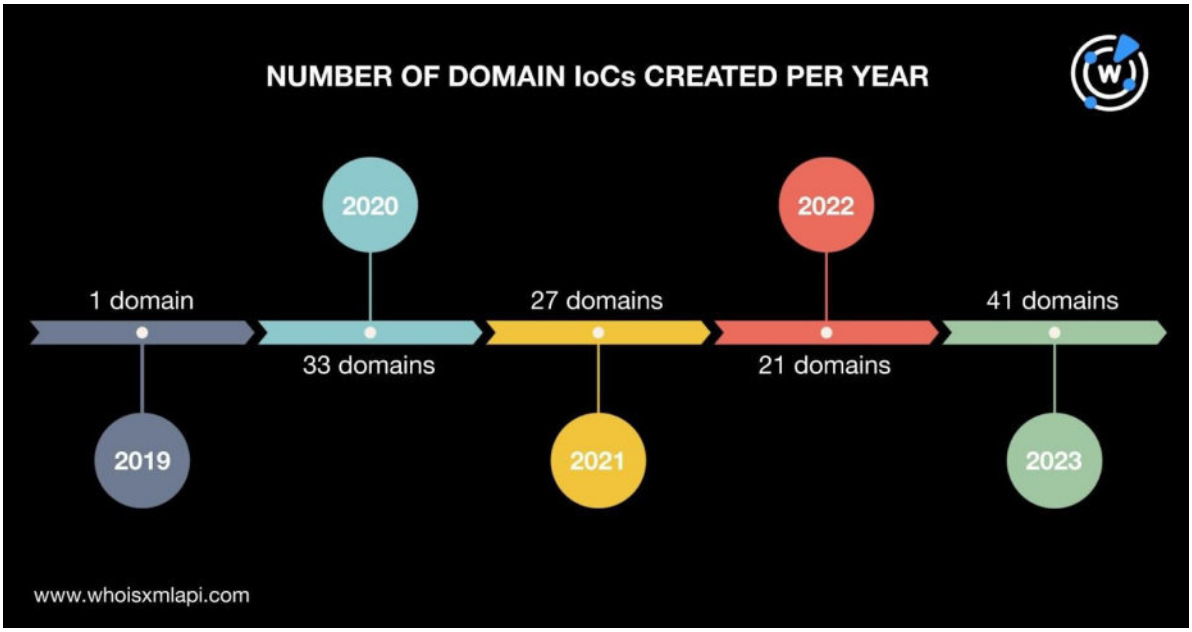
- PAPERWALLのドメインIoCと同じメールアドレスを使用しているドメイン名681個
- IPアドレス1個
- IPアドレスIoCによってホストされているドメイン名1個
- ドメインIoCと同じ文字列を含むドメイン名193個。そのうち1個は悪意あるドメイン名

DNSにおけるPAPERWALL IoCの実態

まず、PAPERWALLのIoCに関する情報を集めることにしました。123個のドメインIoCをBulk WHOIS Lookupにかけたところ、以下のことが判明しました：

- 全てGoDaddy.com LLC経由で登録されたドメイン名でした。

- 全て2019年から2023年の間に新規登録されたものでした。41個は2023年、33個は2020年、27個は2021年、21個は2022年、1個は2019年に登録されていました。

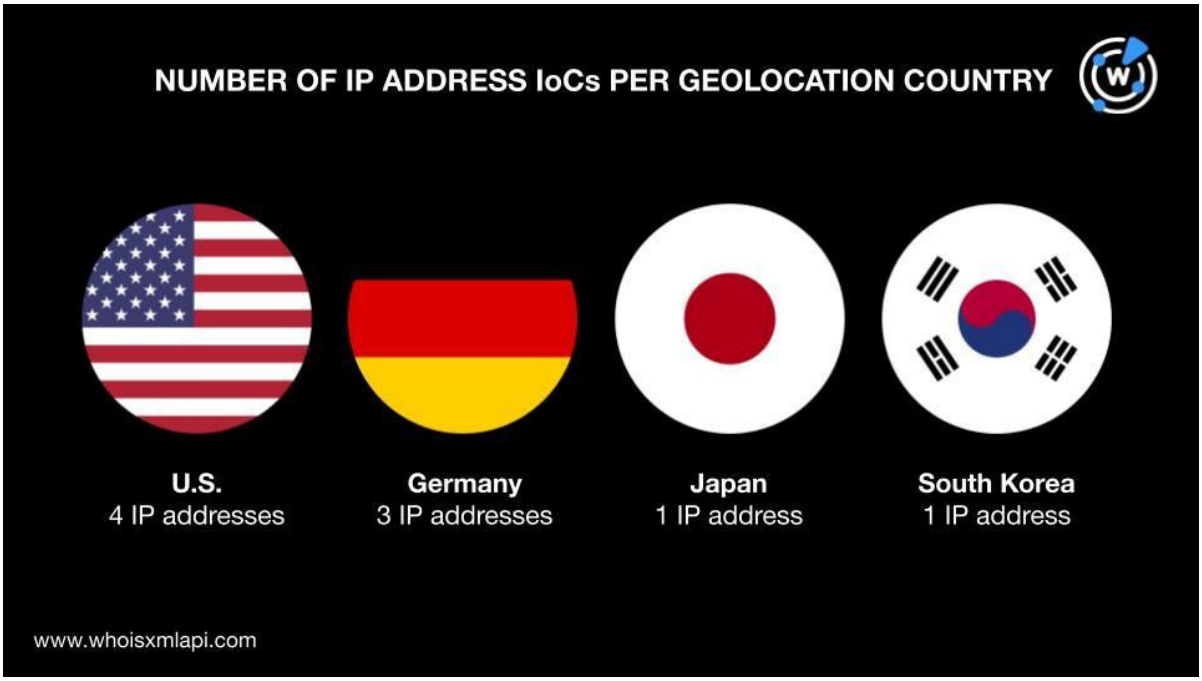


- 122個のドメインIoCは米国で登録されていました。残り1個のドメインIoCについては、現在のWHOISレコードに登録者の国の情報がありませんでした。

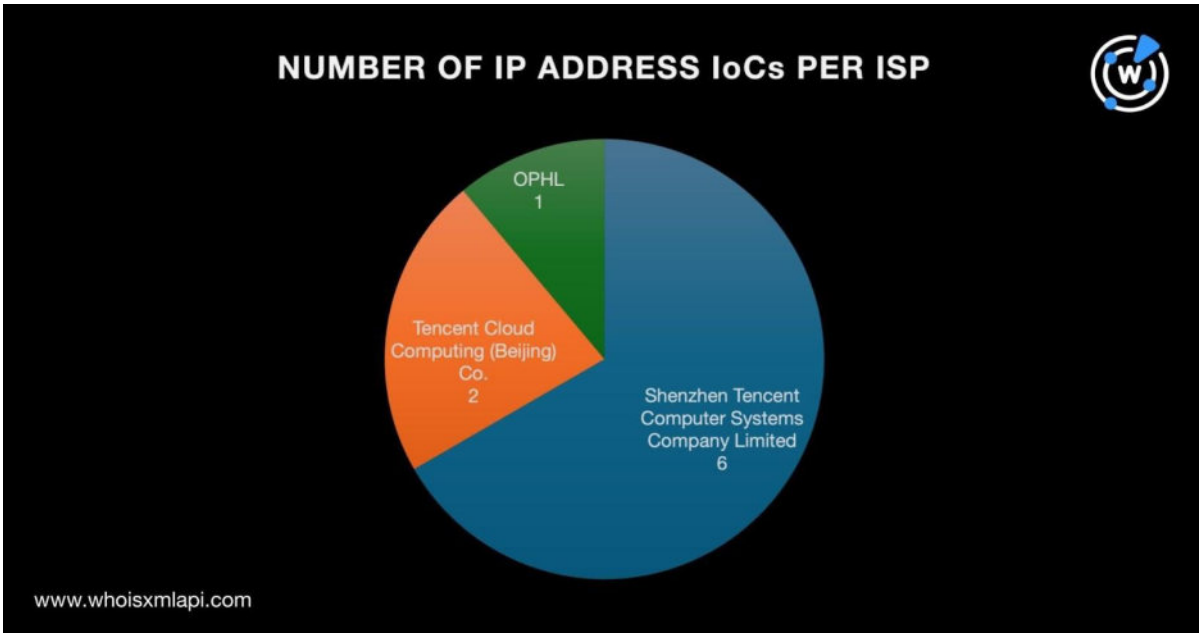
123個のドメインIoCのドメイン名ラベルに最も多く見られたニュース関連のテキスト文字列は**daily**と**post**で、それぞれ9個のドメインIoCに含まれていました。

次に、9個のIPアドレスIoCをBulk IP Geolocation Lookupにかけたところ、以下が明らかになりました：

- 4個は米国、3個はドイツに位置していました。また、日本と韓国を指すIPアドレスIoCが1個ずつありました。



- Shenzhen Tencent Computer Systems Company LimitedというISPが最多の6個を管理していました。次に管理しているIPアドレスが多かったISPはTencent Cloud Computing (Beijing) Co.で、2個でした。また、OPHLが1個を管理していたことがわかりました。



PAPERWALL IoCと関わりを持つアーティファクトを探索

PAPERWALLとの関連性を持つ未報告のアーティファクトを特定するため、123個のドメインIoCを用いてWHOIS History APIで検索を実行しました。そして、過去のWHOISレコードから、合計56個（重複を除く）のメールアドレスを検出することができました。なお、そのうち33個は無編集のまま公開されていました。

その33個の公開メールアドレスを検索語としてReverse WHOIS APIで現在のWHOISレコードを調べたところ、33個のうちいずれかのメールアドレスを共用していたドメイン名が681個（重複および既存IoCを除く）見つかりました。

681個のうち103個は、ドメインIoCと同様にニュース関連の文字列を含んだドメイン名でした。また、103個のうち64個には、新聞を指して使われるスペイン語の**diario**（「日誌」「日刊紙」の意）という文字列が見られました。その他、以下のようなニュース関連のテキスト文字列がドメイン名の中に見つかりました：

- **critic**
- **daily**
- **desk**
- **dia** (Spanish word for “day”)
- **global**
- **government**
- **journal**
- **magasin** (Filipino word for “magazine”)
- **magazine**
- **monthly**
- **paper**
- **periodico** (Spanish word for “newspaper”)
- **press**
- **radio**
- **television**
- **today**
- **video**
- **weekend**
- **writer**

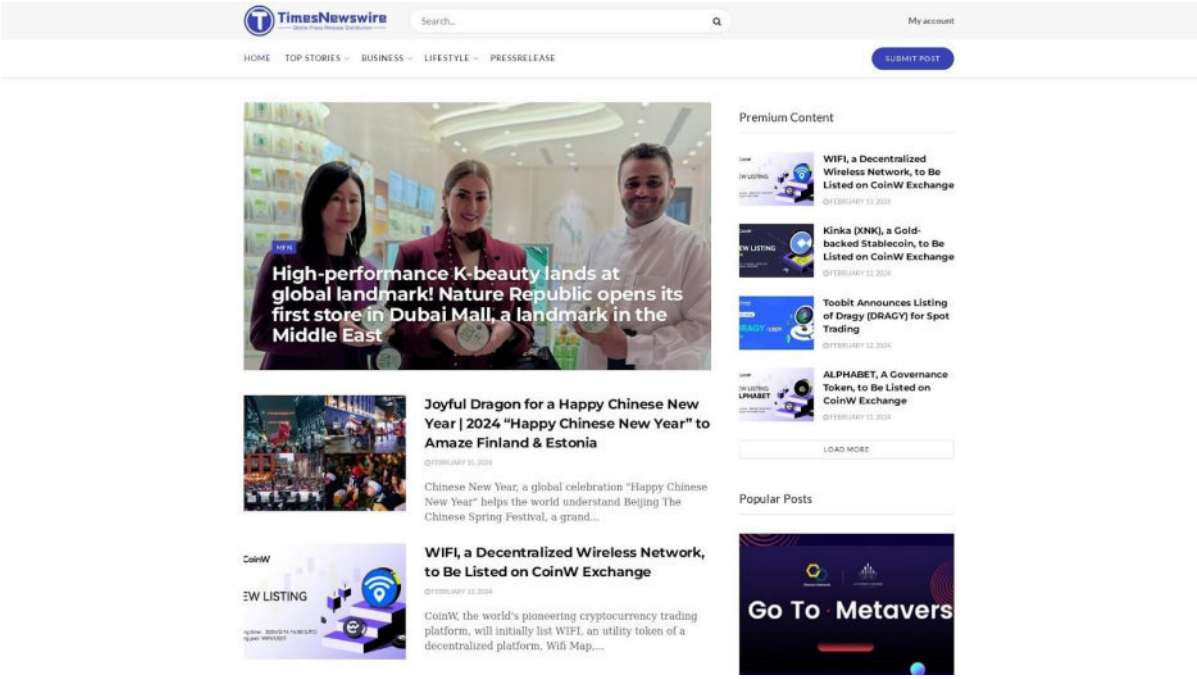
しかし、ドメインIoCと同じメールアドレスを共用していたドメイン名の中に、ドメインIoCで最も多く見られた文字列の一つである**post**を含んだものはありませんでした。

また、Screenshot APIを実行した結果からは、ドメインIoCと同じメールアドレスを共用していたドメイン名のうち7個が有効なページを指していたことが確認されましたが、いずれもニュースフィードではありませんでした。

次に、123個のドメインIoCをDNS Lookupにかけたところ、1個のIPアドレス（128[.]14[.]74[.]124）が新たに検出されました。そのアドレスのジオロケーションは大部分のIPアドレスIoCと同様に米国でしたが、管理ISPはIPアドレスIoCのそれと異なり、Zenlayer, Inc.でした。

既存の9個のIPアドレスIoCと今回の調査で新たに検出した1個のIPアドレスを使ってReverse IP Lookupで検索した結果、そのいずれかを使用していた1個のドメイン名（timesnewswire[.]com）

が特定されました（重複、IoCおよびドメインIoCと同じメールアドレスを共用していたドメイン名を除く）。The Citizen LabとMandiantによれば、このドメイン名はHaiEnergyが攻撃で使用したものです。現在もアクセス可能で、最新ニュースをホストし続けています。



timesnewswire[.]comのスクリーンショット

最後に、Domains & Subdomains Discoveryを使い、ドメインIoCに見られる以下のいずれかの文字列を含むドメイン名を探しました：

- **alpsbiz.**
- **bohemiadaily.**
- **cctimes.**
- **cordovapress.**
- **dkindustry.**
- **doloreshoy.**
- **euleader.**
- **friendlyparis.**
- **fukuoka-ken.**
- **gwangjuedu.**
- **kanagawa-ken.**
- **kazanculture.**
- **londonclup.**
- **louispress.**
- **nlpress.**
- **romajournal.**
- **rostovlife.**
- **saitama-ken.**
- **samaraindustry.**
- **sanrafaelscoop.**
- **seoulpr.**
- **stptb.**
- **updatenews.**
- **usa-aa.**
- **vikingun.**
- **volgogradpost.**
- **vtnay.**
- **wakhan.**

- **wdpp.**

検索結果から重複、IoC、ドメインIoCと同じメールアドレスを共用しているドメイン名を除いたところ、上記のいずれかの文字列を含むドメイン名が193個見つかりました。そのうちの1つであるupdatenews[.]meは、Threat Intelligence APIの結果から、マルウェア攻撃と関連していることがわかりました。

Screenshot APIで調べたところ、本稿執筆時点で193個のうち57個のドメイン名はアクセス可能な状態にあります。また、193個中17個はニュースフィードのような見た目のページにつながりますが、そうしたページはプロパガンダの拡散に悪用されている可能性があります。

その他のニュース関連ドメイン名の兆候

先述の通り、ドメインIoCおよびドメインIoCと同じメールアドレスを共用していたドメイン名に最も多く見られたニュース関連のテキスト文字列は、**daily**、**post**、**diario**の3つです。しかし、**post**は郵便サービスに関連するドメイン名にも含まれている可能性があるため、ここではPAPERWALLのドメインIoCと同じようなウェブサイトをホストしている可能性が高い**daily**と**diario**のみに注目しました。

Domains & Subdomains Discoveryで検索した結果、2024年1月1日以降、**daily**を含むドメイン名が5,277個新規登録されていることがわかりました。そして、Threat Intelligence APIの結果から、そのうち5個は悪意あるドメイン名と確認されました。5個のうち4個はフィッシングに、残りの1個はマルウェア攻撃に関連していました。

他方、2024年1月1日以降に新規登録された**diario**を含むドメイン名を検索したところ、289個のドメイン名が該当しました。

—

現在進行中のPAPERWALLというプロパガンダキャンペーンに関与した132個のIoCを詳しく調べた結果、潜在的な関連アーティファクトが合計876個（ドメインIoCと同じメールアドレスを使用しているドメイン名681個、IPアドレス1個、IPアドレスIoCによってホストされているドメイン名1個、ドメインIoCと同じ文字列を含むドメイン名193個）発見されました。今のところ、そのうち悪意あるものと確認されたのはドメインIoCと同じ文字列を含むupdatenews[.]meというドメイン名のみですが、他のアーティファクトも誤情報の拡散に悪用される可能性があります。

また、**daily**と**diario**というたった2つの文字列を足がかりに、PAPERWALLと同様の悪意ある活動に関わった可能性がある何千ものドメイン名を特定することができました。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：関連アーティファクトの例

ドメインIoCと同じメールアドレスを使用していたドメイン名の例

- 0500london[.]org
- 0800london[.]org
- 121w[.]org
- 17tvmall[.]org
- 17tvos[.]org
- 24hourlondon[.]org
- 865623333[.]org
- aberdeenairporthotels[.]org
- acabadosaeroprint[.]com
- accaoimediata[.]pt
- accommodationlondon[.]org
- aceitetorredonjimeno[.]com
- adegcostadelsol[.]com
- aircmosventas[.]com
- alimentacioneuropea[.]com
- americaaffiliate[.]org
- americadata[.]org
- americaexperts[.]org
- americaknowledge[.]org
- americamaps[.]org
- andalucia[.]catering
- andalucia[.]consulting
- andalucia[.]sexy
- andaluciagay[.]org
- approbuilder[.]com
- apvherreriaalex[.]com
- artebird[.]info
- artedemarruecos[.]com
- artetheadbird[.]info
- artslondon[.]org
- attractionslondon[.]org
- auctionscostadelsol[.]com
- autocaresluna[.]mobi
- axbz[.]org
- bailegay[.]com
- barneshotels[.]org
- bddos[.]org
- bedfordshirehotels[.]org
- benidormhomosexual[.]com
- berkshirehotels[.]org
- besthighchair[.]org
- bexleyhotels[.]org
- biarritzgay[.]com
- bitxigarbiketak[.]com
- bjzyz[.]org
- blackheathhotels[.]org
- bogotagay[.]org
- bomberosmagazine[.]com
- brentfordhotels[.]org
- britaindata[.]org
- britainmarketing[.]org
- britainuniversities[.]org
- budgetlondon[.]org
- campeonatodelmundodecine[.]com
- campeonatodelmundodefilms[.]com
- carnicascarrion[.]com
- carpinteriabasalum[.]com
- carpinteriafranciscosoriano[.]com
- carpiteriametalicaperez[.]mobi
- carrentallondon[.]org

- carskiss[.]com
- casamasip[.]mobi
- casaruralogonomendi[.]com
- centraldecomprasgays[.]com
- centroeuropeodecongresos[.]com
- certamendebomberos[.]com
- chinaseafood[.]org
- chingfordhotels[.]org
- chislehursthotels[.]org
- chiswickhotels[.]org
- chlgrupo[.]net
- cinegaycostadelsol[.]com
- circulofinancierointernacional[.]com
- claphamhotels[.]org
- clevelandsurvey[.]org
- clinicadentalgabrielrubio[.]com
- cnrmb[.]org
- coachcompanies[.]org
- coches56[.]com
- cofradiasenred[.]com
- colegatorremolinos[.]com
- comemelapolla[.]org
- comerhoy[.]net
- contenedoresurbil[.]com
- conventionlondon[.]org
- cordesalinas[.]com
- cortijoaltozano[.]com
- cpdesk[.]ca
- cpdesk[.]us
- croftonpark[.]org
- crouchend[.]org
- crystalpalacehotels[.]org
- cubiertasmiguelmartinez[.]com
- cubiertasytejadosdepizarraenasturias[.]com
- cundian[.]org
- customrubixcube[.]org
- dailylondon[.]org
- derbyshirehotels[.]org
- desguaceluqueislamayor[.]com
- desinsectacionesenmarbella[.]com

ドメインIoCと同じ文字列を含むドメイン名の例

- alpsbiz[.]site
- bohemiadaily[.]cz
- bohemiadaily[.]eu
- cctimes[.]ca
- cctimes[.]cc
- cctimes[.]club
- cctimes[.]cn
- cctimes[.]co[.]kr
- cctimes[.]co[.]uk
- cctimes[.]com
- cctimes[.]com[.]au
- cctimes[.]com[.]cn
- cctimes[.]date
- cctimes[.]gift
- cctimes[.]help
- cctimes[.]info
- cctimes[.]kr
- cctimes[.]link
- cctimes[.]mobi
- cctimes[.]net
- cctimes[.]net[.]cn
- cctimes[.]news
- cctimes[.]online
- cctimes[.]pub
- cctimes[.]ren
- cctimes[.]site
- cctimes[.]tech
- cctimes[.]top
- cctimes[.]vip
- cctimes[.]win
- cordovapress[.]com
- dkindustry[.]co[.]kr

- dkindustry[.]co[.]za
- dkindustry[.]com
- dkindustry[.]in
- dkindustry[.]net
- dkindustry[.]org
- doloreshoy[.]com
- euleader[.]com
- euleader[.]com[.]br
- friendlyparis[.]fr
- friendlyparis[.]org
- friendlyparis[.]xn--fiqs8s
- friendlyparis[.]xn--fiqz9s
- fukuoka-ken[.]jp
- gwangjuedu[.]co[.]kr
- kanagawa-ken[.]jp
- kanagawa-ken[.]net
- kazanculture[.]ru
- londonclup[.]xyz